

Key Takeaways

- To turn Stolen Device Protection on or off, Go to **Settings** > **Face ID & Passcode** > Enter your device **passcode** > **Stolen Device Protection** > Turn **on/off toggle** switch next to Stolen Device Protection.
- Stolen Device Protection prevents thieves from changing sensitive information, even if they somehow learn your iPhone's passcode.
- It uses your iPhone's location to determine if the iPhone is not in a familiar location, making the Face ID authentication necessary for sensitive changes.
- You can also set the security delay to stay active always regardless of location if you want increased security.

Since iPhones are popular and expensive, they often get stolen. Although Find My helps locate your device, it doesn't ensure your iPhone's data is safe from thieves. Apple has released a new feature called Stolen Device Protection with iOS 17.3 to cope with this issue and secure your data in case of theft.



In this article, I will explain how to turn on or off Stolen Device Protection on your iPhone and how it works.

What is Stolen Device Protection for iPhone, and how does it work?



Stolen Device Protection is an additional layer of security that prevents anyone from changing sensitive information on your iPhone. When [stolen](#), the thief won't be able to access any of your private data without Face ID/Touch ID.

It's an extra security toggle that protects your iPhone against specific thefts. Once enabled, it's hard for someone to alter your iPhone's data even if they stole your iPhone knowing your passcode.

The [Wall Street Journal](#) reported a disturbing trend in iPhone thefts. Thieves were using long-range cameras to capture users entering their passcodes in public, later exploiting this information to alter Apple ID settings and access financial accounts.

With Stolen Device Protection enabled the iPhone asks for Face ID/Touch ID when accessing or changing sensitive information, such as Apple ID passwords, saved passwords, auto-fill card details, and more.

Suppose someone other than you tries to change your Apple ID password. In that case, the system will ask for your Face ID/Touch ID and will also start a one-hour timer, after which it'll ask the user to provide a valid Face ID/Touch ID again.

When turned on, Stolen Device Protection won't affect your usage. If your iPhone remembers your significant locations, such as home or work, it won't ask for this extra layer of protection.

We hope this doesn't happen, but when your iPhone gets stolen, here's what the thief can't do on your iPhone:

- Access your saved passwords
- Auto-fill your card or payment details in Safari
- Turn off Lost Mode
- Erase all contents & settings
- Apply for a new Apple Card
- View Apple Card virtual number
- Few Apple Cash/Savings Actions
- Set up new devices
- Turn off Stolen Device Protection

Requirements to use Stolen Device Protection

If you want to turn on Stolen Device Protection, you need to ensure that your iPhone meets these requirements:

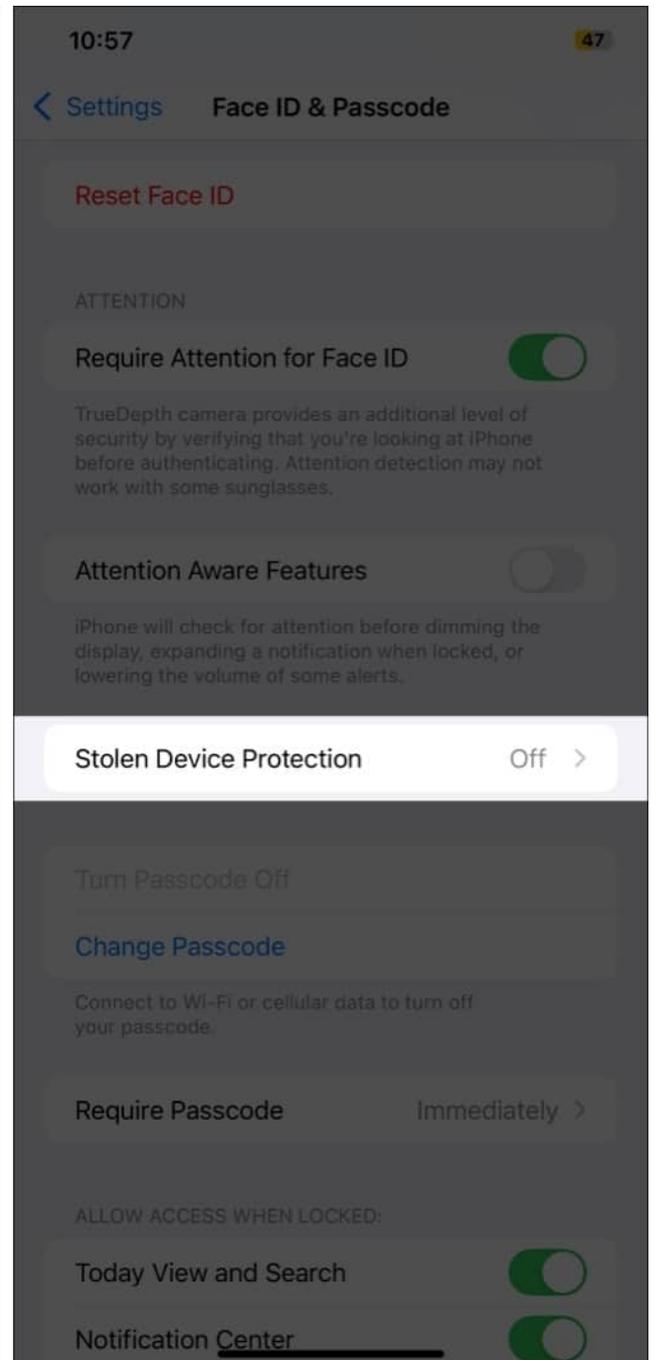
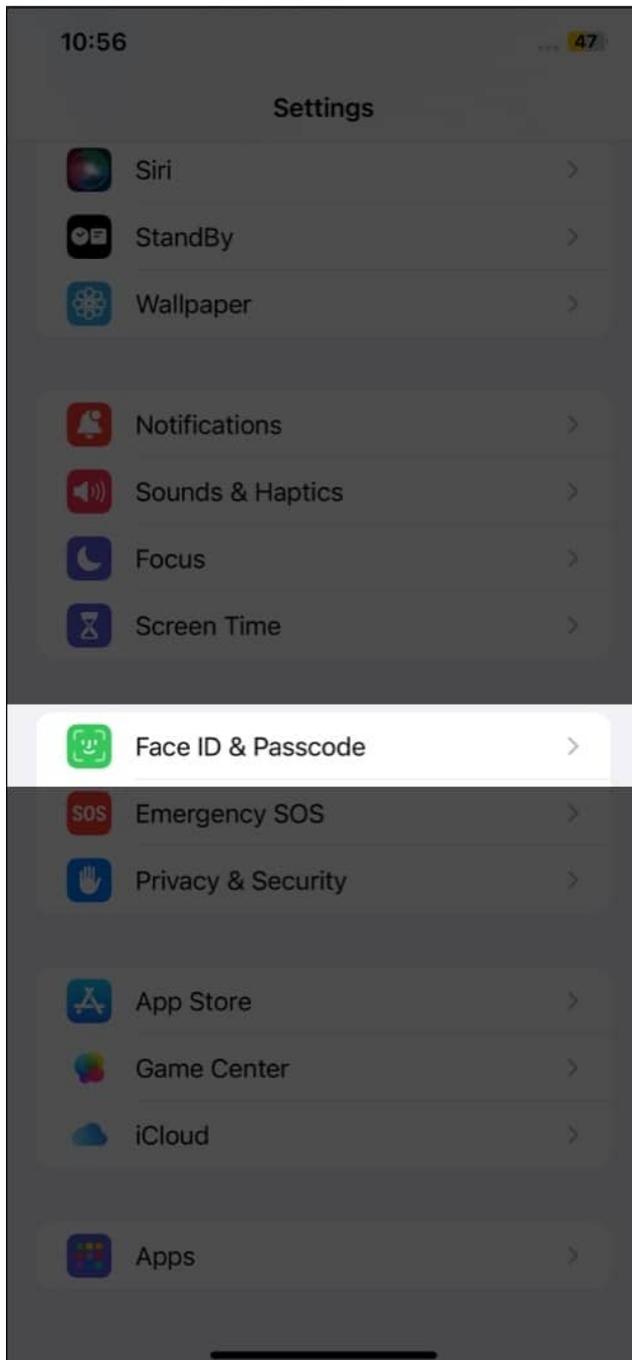
- Your iPhone should be running iOS 17.3 or above.
- 2FA (Two-Factor Authentication) set up for Apple ID
- Device Passcode turned on
- Face ID/Touch ID enabled
- Find My enabled

Plus, if you have significant locations (such as Home or Work) set up, it can be beneficial.

How to enable or disable Stolen Device Protection on iPhone

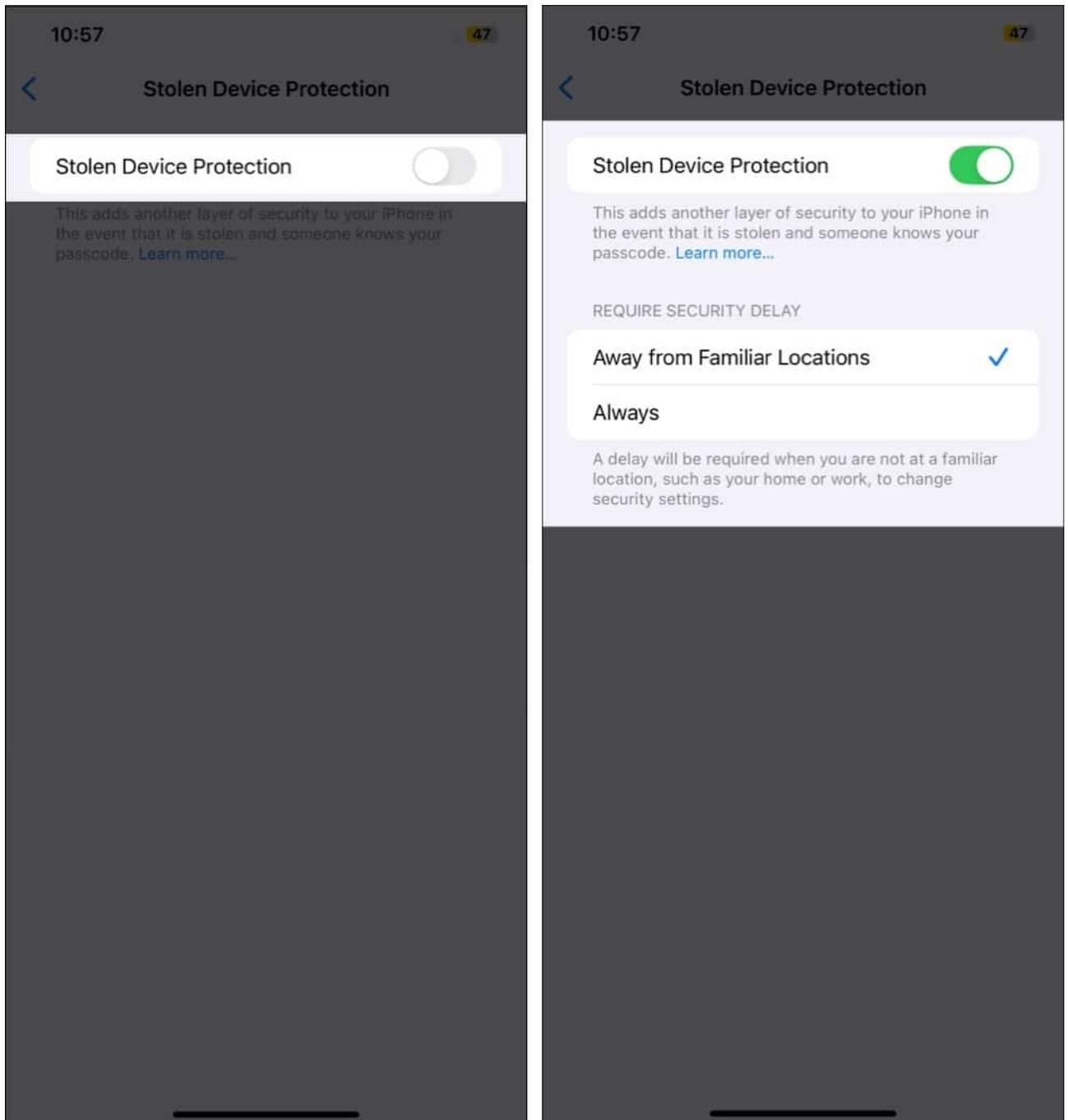
1. Open the **Settings** app and tap **Face ID and Passcode**.

2. Enter your device **passcode** and tap **Stolen Device Protection**.



3. Now, **toggle on** Stolen Device Protection.

4. Next, select whether you want the Security Delay to be required only when the iPhone is away from a familiar location or always.



Later, if you don't want to use it, turn off **Stolen Device Protection**.

Stolen Device Protection Enhances Security...

Apple's Stolen Device Protection is a valuable feature that [enhances your iPhone's security](#)

when detected in unfamiliar locations. Your data will remain safe even if someone gets their hands on your iPhone and knows your iPhone's Password.

We recommend you enable Stolen Device Protection to prevent thieves from stealing information from your iPhone. If you have any other queries or suggestions regarding this guide, please leave them in the comment section below.

Read more:

- [6 Tips to Secure your iPhone and iPad Lock Screen](#)
- [How to check iPhone Activation Lock status online](#)
- [How to Set up Two-Factor Authentication \(2FA\) for Apple ID](#)
- [12 iPhone security and emergency features you should start using](#)